ERGONOMICALLY DESIGNED MULTIFUNCTIONAL TRANSACTION TERMINAL

Field of the Invention

The invention relates to data collection devices and more particularly to a transaction terminal for use in aiding purchase transactions and other transactions.

Background of the Prior Art

"Transaction terminals" of the type having a data collection (e.g. mag stripe, smart card) input and signature capture capability for attachment to a point-of-sale (POS) network are growing in popularity. Unfortunately, currently available transaction terminals have been observed to exhibit numerous limitations.

For example, while presently available transaction terminals often are configured to prompt a user to enter personal identification (PIN) information, presently available transaction terminal lack adequate security features for assuring that the PIN information cannot be stolen, either by overriding of an encryption routine or by theft of encryption keys.

Presently available transaction terminals are also lacking in security features for monitoring presentation fraud. For example, while transaction terminals prompt a user to enter PIN information and to enter a signature, they are lacking in features which would enable determination of whether the person presenting information is in fact the person he purports to be.

The physical housings presently available transaction terminals have also observed to be problematic. The reading unit of presently available transaction terminals is a "swipe" style mag strip card reader which defines a slit opening on the top of the terminal. The orientation and configuration of

these swipe-style slot transaction terminals force a reader into assuming uncomfortable and awkward body and arm positions during the reading process.

Other problems with present day transaction terminals exist as well. For example, present day transaction terminal allow unscrupulous persons to open the terminal, and remove secure information bearing microchips or to syphon information from the chips.

There is a need to address these and other problems observed with presently available transaction terminals.

Summary of the Invention

According to its major aspects and broadly stated the invention is an ergonomically designed multifunctional transaction terminal for use in various transactions such as transactions involving credit cards, debit cards, and customer loyalty cards.

A transactional terminal according to the invention in one possible embodiment includes a housing having a top portion partially defined by a touch screen, a base, and an enlarged head portion extending forwardly from the base to define a lip. An insert style card reader having horizontally oriented feed slot opening toward the front of the housing is disposed in the lip of the housing. The feed slot may be angled downward slightly to reduce build up in the slot and to encourage a sweeping action on the part of a card during card removal. The touch screen may be angled downward in coplanar relationship with the feed slot to improve visibility of the touch screen and to improve simultaneous observation of touch screen and card indicia. The housing may include a detachable riser and may be adapted to receive a detachable holder

apparatus for holding a stylus.

The transaction terminal according to the invention may further include numerous other features including a secure information entry circuit, a tamper detection security feature, an improved data I/O system, and an improved user interface system.

These and other details and advantages will become apparent from the detailed description of the preferred embodiment hereinbelow.

Detailed Description of the Drawings

Figs. 1a and 1b are perspective views of an exemplary transaction terminal according to the invention;

Fig. 1c is a top view of an exemplary transaction terminal according to the invention;

Fig. 1e is a side view of an exemplary transaction terminal according to the invention;

Fig. 1f is a side view of a wedge style user according to the invention;

Fig. 1g is a bottom perspective view of a transaction terminal according to the invention;

Figs. 1h and 1i are cutaway side views of an exemplary transaction terminal according to the invention;

Figs. 1j and 1k are bottom perspective views of an exemplary transaction terminal according to the invention having SAMS access doors;

Figs.1L an 1m is a terminal according to the invention including an integrated fingerprint scanner.

Fig. 1n shows a universal cable of the invention;

Fig. 1o is a top view of a universal connection of the invention;

Fig. 1p is a side view of a terminal including an optical reader;

Fig. 1q is a front view of a terminal according to the invention including an optical reader, a retinal scanner and a fingerprint scanner;

Fig. 1r is a perspective view of a riser.

Figs. 1s-1t are view of terminals in an exemplary embodiment for illustrating dimensional features.

Fig. 2a is a functional electrical block diagram of an exemplary transaction terminal according to the invention;

Fig. 2b is an exemplary chip system architecture diagram of an exemplary transaction terminal according to the invention;

Fig. 2c is a functional electrical block diagram showing of a security block shown in the block diagram of Fig. 2a;

Fig. 2d shows an alternative embodiment of a security block according to the invention;

Fig. 2e shows a functional block diagram of a secure information entry circuit of the invention;

Figs. 2f and 2g are memory maps illustrating just two of several possible embodiments of firmware;

Fig. 2i is a flow diagram illustrating an exemplary encryption routine according to the invention.;

Fig. 3a is a flow diagram illustrating a flow of events in a typical POS transaction;

Figs. 3b-3e show various embodiments of possible POS networks;

Figs. 3f-3g illustrate alternative cash registers which may be disposed in communication with a transaction terminal of the invention;

Fig. 4a is an exemplary assembly diagram for an exemplary

transaction terminal according to the invention;

Figs. 4b and 4c are detailed assembly diagrams illustrating a break-in detection feature according to the invention;

Fig. 4d is a partial exploded perspective view of a main PCB of an exemplary transaction terminal according to the invention;

Fig. 5a is a side view of an exemplary stylus and cord according to the invention;

Fig. 5b is a cutaway partial side view of the stylus shown in Fig. 5a;

Figs. 5c, 5d, and 5f are perspective views of a stylus holder assembly according to the invention;

Fig. 5e is a side view of a holder assembly according to the invention;

Figs. 6a-6e are various perspective views of a hybrid reader unit which may be incorporated in a transaction terminal according to the invention;

Figs. 7a-7b are functional diagrams illustrating a brooming effect of the invention;

Fig. 7c is a business model diagram illustrating a method for marketing ad supplying a terminal according to the invention;

Figs. 8a-8b are function lay-out diagrams of a ouch screen overlay;

Fig. 9 illustrates a prior art transaction terminal.

Detailed Description of the Invention

Perspective views of a transaction terminal according to the invention, which may be adapted for reading card information, for secure receipt of personal identification

(PIN) information, for signature capture, and numerous other functions are shown in Figs. 1a, 1b, and 1g. Card 90 which is processed by transaction terminal 10 may be, for example, a credit card, a debit card, customer loyalty card, an electronic benefits card, a company-sponsored benefits card, an identification card, etc.

Transaction terminal 10 includes a rugged housing 11 having a top 11a, a bottom 11b, a front 11f, and sides 11s. Housing 11 further includes a base portion 11bs and an enlarged head portion 11h extending forwardly from base 11b to define a lip 11L. Integrated in the top 11T of terminal is a touch screen 20, which will be described herein, comprises a display 234 and a touch sensitive overlay 23 disposed over display 234. Disposed in housing lip 11L and opening toward front 11F of housing 11 is an insert-style card reader 240. Housing 11 further includes a detachable riser 11R and a tangle-resistant stylus 30 disposed in a specially configured holder apparatus 40 adapted for attachment either on housing 11 or on another member separate from housing 10. Terminal 10 further includes I/O connection ports 40 and 42 for allowing communication with other computer systems such as cash registers, or other host computer systems, e.g server system, or hub computer systems as will be described later herein.

A high level electrical block diagram of terminal 10 is shown in Fig. 2a. Terminal 10 includes a control circuit 210 which typically comprises at least one IC microchip. For example, an Intel 133 MHz or 206 Mhz SA-1110 Strong-arm CPU is suitable for use in circuit 210, although faster and less expensive CPU IC's will be preferred when they become available. In addition to having a central processing unit, CPU 212, control circuit 210 further includes a memory 216

typically having at least RAM 217 and ROM 218 memory devices. ROM 218 may be a reprogrammable ROM, otherwise known as a "flash" ROM.

Control circuit 210 may be in communication with other types of of memory including "flash" type memory, e.g. a memory device 216F sold under the commercial names "Multimedia MMC," "Smart Media," "Compact Flash," and "Memory Stick." Flash type memory devices are especially useful for storing image data and signature data. Memory 216 which may be included in or in communication with control circuit 210 may also comprise a long term storage device 216s such as a hard drive, a floppy disk, or a compact disc. It has become increasingly common to package memory devices, particularly RAM and ROM devices within a single IC chip including control circuit CPU 212, RAM 216, and ROM 218.

Control circuit 210 is in communication with a number of components, including reader unit 240 which in a preferred embodiment in an insert style (also known as "dip" style) hybrid magnetic stripe and smart card reader/writer. Hybrid reader 240 may be an OEM integrated unit, e.g. a ZU series reader of the type available from Matsushita of Japan, an ST-40 series hybrid reader available from Secure-Tech, or a hybrid reader of the type available from IDTECH. Hybrid reader unit 240 includes a mag stripe reader 241 in communication with magnetic control and decode circuit 242, and smart card reader/writer 243 in communication with smart card control and decode circuit 244. Hybrid reader unit 240 may be disposed in pocket 13 defined in lower section 11LW of housing 11 as seen in assembly view Fig. 4a.

Control circuit 210 in the embodiment of Fig. 2a is also in communication with an RF ID reader unit having a reader

261, with associated control and decode circuit 262. RF ID reader 261 may be, for example a Kronegger miniaturized RF reader, readily connected to PCB 290, having a 25x35 mm footprint and power consumption below 100ma reader may be mounted just under housing upper portion 261p indicated in Fig. 4L.

Another user interface data input device which may be disposed in communication with control circuit 210 is an optical reader unit having imaging assembly 263 and associated control and decode out circuit 264. Decoding could also be carried out by control circuit 210. A model IT 4200 optical reader module with decode out circuit of the type available from Hand Held Products, Inc. may be selected to provide the function indicated by blocks 263 and 264. Assembly 263 could also be a linear assembly. Embodiments of transaction terminals according to the invention including an optical reader unit having 263 are shown in Figs. 1p and 1q. Assembly 263 is readily installed in side 10s of base 10bs. More particularly housing 11 can include an imaging assembly aperture for accommodation of imaging assembly 263. The aperture may accommodate assembly 260 by allowing light to pass through the imaging assembly aperture in the case assembly is mounted entirely inside housing 11 or may accommodate assembly 263 by allowing a part of assembly 263 to extend into the exterior of housing 11 in the case assembly 263 is mounted in such a manner that it is disposed partially inside and partially outside of housing 11. The height of the integrated portion of base 10bs may be increased as shown so that e.g. a credit or debit or identification card is readily placed in the field of view of reader 236.

It will be appreciated that significant functionality is

added to terminal 10 when terminal is equipped with an optical reader. When terminal 10 includes a 2D reader control circuit 210 can store frames of image data into memory e.g. memory 216f. Optical reader 263 can be controlled for use in capturing frames of image data comprising handwritten signatures. If control circuit 210 determines that a signature capture mode using touch screen 20 fails, control circuit 210 may display a prompt prompting a user to dispose a signature bearing substrate in the field of view of imaging assembly 263. Circuit 210 may further display on screen 20 a button for actuating image capture, then capture a signature when a user actuates a control button. By storing the image representation including a signature representation into memory 216. The symbol decoding functionality of reader unit including assembly 263 coupled with the image capture functionality of assembly 263 renders terminal 10 operable to execute numerous types of user-interactive methods which are useful for fraud prevention and other purposes. U.S. Serial No. 09/788,179, entitled "Identification Card Reader" filed February 16, 2001, and assigned to the assignee of the present invention describes numerous methods for determining whether a card holder is the person he purports to be utilizing an optical reader having image capture and decode capability and numerous other methods relating to identification and fraud prevention. Applicants hereby expressly incorporate herein U.S. Serial No. 09/788,179 in its entirety by reference. It is seen from Fig. 1q that terminal 10 may include a card holding tray 19 for holding an identification card in the field of view of assembly 263 such as the identification card reader card holder described in detail in the above mentioned U.S. Serial No. 09/788,179 application.

Still further, control circuit 210 may be in communication with a fingerprint scanner unit having a scanner 265 and associated control circuitry 266. A fingerprint scan unit may be provided by, for example, by a BERGDATA OEM module fingerprint scan unit or an ULTRA SCAN Corp. Series 400 OEM Fingerprint Scan unit. Transaction terminal 10 may capture an electronic fingerprint representation and send the electronic fingerprint representation to a non-integral computer system such as a computer system of Network 380, and Network 380 may perform the identification. Also Network 380 may periodically download a database of relevant electronic fingerprint authorizations for use by control circuit 210 in performing fingerprint identification functions. Transaction terminals according to the invention comprising integrated fingerprint scanning units are shown in Figs. 1L, 1m, and 1q. Scanner 265 may include finger receiving recess 265r integrally formed in housing 11. Scanner sensor 265 may be disposed under a window formed in bottom surface of recess 265f. A fingerprint scanning unit according to the invention can also comprise an insert-stylus finger scanning unit.

Transaction terminal 10 can also include a retinal scan unit including scanner 267 associated control circuit 268. A scan unit including scanner 267 and control circuit 268 may be provided by components from an Icam 2001 retina scan unit available from Eye Dentify Corp. Control circuit 210 may perform identifications based on captured retinal scan signatures by transmitting captured electronic retinal signatures to a nonintegrated computer system for identification, e.g. to Network 380, or by downloading a database of signatures from e.g. Network 380 for identification by circuit 210. A retinal scanning transaction

terminal 10 is shown in Figs. 1m, 1p, and 1q showing a terminal having a retinal scanner 267 including a retinal scanner eyepiece 267e integrally formed in terminal housing 11.

Transaction terminal 10 further includes a touch pad screen 20 including a display 234 and a touch pad overlay 230. Touch pad screen or "touch screen" 20 displays information to a user such as prompt information, a virtual keypad, and advertising messages, etc. Touch screen 20 also serves as a means to input data. Touch screen 20 serves as both a virtual keypad and signature capture platform. Touch pad screen 20 may comprise an LCD display 234 in combination with a touch screen overlay 230. Display 234, e.g. may be a 5.7", 1/4 VGA (320x240) resolution color or monochrome LCD screen of the type available from Nan Ya Corporation. Display 334 may be driven by an on-chip LCD controller available on a microchip including circuit CPU 212 if circuit is appropriately selected, or in association with dedicated control circuit 235 as shown in Fig. 2a. Referring to assembly view of Fig. 4a LCD display 234 may be mounted on LCD bracket 17 which is mounted to housing lower section 11LW.

Touch screen overlay 230 may be, for example, a Nissa NIS/RC-872 overlay with parallel interface. Touch screen overlay 230 typically operates in association with touch screen controller 231. Touch screen control circuit 231, like LCD circuit 235 can be integrated in an IC comprising element control circuit 210. In the embodiment shown in assembly view Fig. 4a, display 234 includes a side-mounted back light unit 236. For increasing the uniformity of illumination, display 234 could include a top-mounted backlight 236 which would occupy positions along top edge 234e of display 234. Display

234 is disposed in housing 11 so that the side mounted back light unit 236 is housed in terminal 10 on a side of terminal 10 opposite reader unit 240. Increasing the distance between backlight unit 236 and mag stripe reader 241 reduces the effect of electromagnetic interference from backlight unit 236. In the specific embodiment described, backlight unit 236 is powered by inverter 237 which converts DC power output by power system 238 into high voltage AC power for powering backlight 236.

As shown in Figs. 8a and 8b and in accordance with a further aspect of the invention, touch screen 20 and more specifically overlay 230 of touch screen 20 may be configured to be divided into zones 806 and 808, wherein zone 808 is optimized for stylus data entry and zone 806 is optimized for entry of information by actuation by a user's finger. Overlay 230 as best seen in a conceptual schematic diagram of Fig. 8a comprises a series of layers 810, 812, and 814, which vary in number depending on the selection (make and model number) of touch screen overlay 230. Touch screen overlay 230 includes a top layer 810, which, as will be described, preferably comprises a single uniform sheet of light transmissive material.

The inventors found that the optimal configuration for touch screen overly 230 varies depending on the intended actuation mechanism for touch screen 20. In certain applications, touch screens are designated for actuation by a finger, in other application stylus 74 and in other applications, such as in terminal 10, both. Touch screen overlays comprise support mechanisms known as "microdots" 820 which are interposed between two layers of overlay 230 as best seen in Fig. 8a. The inventors found that the positioning of microdots 820 which optimizes overlay 230 for receipt of

finger-entered data is not the same positioning which optimizes overlay 230 for stylus-entered data. Notably, the inventors found that in order to optimize touch screen 20 for finger-entered information, microdots 820 should be spaced to a larger average spacing distance than in a touch screen optimized for stylus-entered data.

In the invention described with reference to Figs. 8a and 8b touch screen 20 is divided into two zones, a finger entry zone 806 and a stylus entry zone 808. Preferably stylus entry zone 808 is located forwardly of finger entry zone 806 in terminal 10 as seen in Fig. 8b so that a user can readily view a virtual keyboard displayed in finger actuated zone 806, or other display messages of touch screen 20 in zone 806 while entering signature information into stylus entry zone 808. In finger actuation entry zone 806, as shown by Figs. 8a and 8b, microdots 820 are spaced to an average spacing distance that is larger than in stylus entry zone 808, wherein microdots 820 are spaced closer together than in zone 806.

Preferably, the remaining characteristics of overlay 230 remain as they would have been in the absence of the described microdot spacing variation. That is, layers 810, 812, and 814 of touch screen overlay 230 remain single unitary sheets of light transmissive material. Zones 806 and 808 could also comprise separate and x-y dimension spaced apart sections of layering material. However, such a configuration, among other disadvantages would not allow a person entering signature information to exceed the bounds of signature zone during the course of entering signature data and still have the signature data received.

Referring to further components of terminal 10, terminal 10 may include secure circuit block 220, to be described in greater detail herein in communication with circuit 210 for preventing theft of electronically stored information such as

PIN information.

Still further, transaction terminal 10 includes at least one and preferably more than one communication interface for providing communication with an external computer system such as a cash register 340 or a computer system 350 and 360 of a POS network to be described herein. In the specific embodiment shown in the block diagram of Fig. 2a terminal 10 includes an ethernet interface 250, a USB interface 252 an RS485 IBM Tailgate Interface 253, an RS 232 interface 254. Referring to Figs. 3f and 3g, including multiple interfaces in terminal 10 yields important advantages. When transaction terminal 10 is in communication with cash register via cable 60, to be described herein it is common to concurrently connect terminal 10 via line 61 (typically an ethernet line) directly to retailer server 350. Accordingly, data and instructional communications which are beyond the capacity of cash register 340 (which is often a legacy system) to support can be carried out via direct link 61 between server 350 or (if terminal 10 is properly equipped) another computer system e.g. HUB 360, Network 322.

Terminal 10 can also include such interfaces as a PCMCIA interface 255 in communication with a PCMCIA slot connector 44. Slot connecter 44 may receive, for example, an RF communication card, a flash memory card, an optical reader PCMCIA card or other commonly available PCMCIA cards. PCMCIA slot connector 44 may be disposed to be accessible from the outside of housing 11 or else PCMCIA slot connector 44 may be accessible from the interior of housing 11 only. An RF or other wireless type of interface may also be provided in hard-wired communication with control circuit 210, e.g. an IR interface 277, shown in Fig. 2b. Electrical circuitry associated with the above types of components are more commonly being packaged in a packaged IC that comprises

elements of control circuit 210.

In accordance with the invention, several interfaces can be physically packaged to terminate at housing 11 of terminal 10 in a single electrical connector port 42. As will be discussed in greater detail herein transaction terminal 10 is commonly connected in communication with a cash register 340 which is PC based or PC compatible. Cash registers commonly comprise at least one of four major types of communication connector ports: PC USB, IBM retail USB, RS232 or RS485 physical connector ports, each having a different PIN configuration. In accordance with the invention, terminal 10 includes a universal connector port 42 which includes a plurality of pins, wherein at least a first pin or group 51 of pins **P** are in communication with a first type of interface (e.g. USB), at least a second pin or group of pins 52 are in communication within a second type of interface (e.g. RS 232). Universal connector port 42 of terminal 10 may include additional groups of pins in communication with additional types of interface. For example, a third group of pins 53 may be are in communication with a third type of interface (e.g. RS485)certain types of interfaces may be adapted so that pins "P" of universal port 42 are shared. For example, RS 232 and RS 485 interfaces can be adapted so that pins of the interfaces are shared with use of switching circuitry 272 as will be described herein..

When terminal 10 comprises universal connector port 42, a supplier of terminal 10 supplies along with terminal 10 a cable 60 for connection with universal connector 42 which is available in one of N varieties, where N is the number of interfaces that universal connector port 42 is in communication with within terminal 10. Thus, if universal connector port 42 is connected to four different interfaces (RS 232, RS485, IBM retail USB, PC USB), then a supplier 10

will make available cable 60 in one of four varieties. Each variety of cable 60 will have a proximal end connector 61 which interfaces with universal connector 42. Thus, if universal connector is a 15 socket connector, the proximal end of each variety of cable will include a proximal end connector 61 having 15 pins. The varieties of cables will differ in the connector of distal end 62. The first variety of cable will have distal end connector 62 in accordance with the standard connector form of the first type of interface, the second variety of cable 60 will have a distal end connector 62 in accordance with the standard connector format of the second type of interface and so on. A customer will order the appropriate variety of cable from a supplier depending on the type of interface terminal that will be interfaced within a cash register or other host computer system. In the alternative, a supplier may supply each of several cable varieties to a customer and the customer may chose the appropriate cable, and may switch cables if terminal 10 is required to communicate with a different interface. It can be seen that the product supply system including universal connector port 42 and associated customer selected cable 60 greatly reduces the size requirements of terminal back end 11rr. The universal connector and cable product supply system also significantly reduces the cost of terminal 10 without compromising functionality, since it reduces the number of physical connector ports that have to be integrated during assembly at terminal back end 11rr.

In a further aspect of the universal connector port feature of the invention, control circuit, 210 polls the contents of designated interface identifier, or "cable select pins" 42cs pins of connector 42. When the various cables 60 are made, conductors of cable 60 are wired so that the two conductors of cable 60 which supply the interface identifier

pins of interface 42 supply the identifier pins with a unique signature indicative of the interface to which distal end 62 of cable 60 is interfaced with. For example, it will be seen that a set of cables 60 can be configured so that a first variety of cable supplies interface identifier pins of connector 42 with a signature of 00 indicative of an interface of a first type, a second variety supplies a signature of 01 indicative of an interface of a second type, a third variety of cable 60 supplies a signature 10 indicative of an interface of a third type, and a fourth variety of cable supplies a signature 11 of a fourth type when distal end connector 62 is connected to a device. More specifically, cable 60 can be made to provide a signature indicative of the cable type by manufacturing cable 60 of each variation in a complementary fashion with the voltage supply to connector 42 so that the lines of cable 60 interfacing with cable select pins 42cs of connector 42 return a high logic value to control circuit 210, unless the lines interfacing with cable select pins 42cs are connected within the length in cable to ground. Therefore, by grounding out one line that interfaces with a cable select pin 42cs, a logic 0 is returned to the cable pin select. By grounding out both lines of cable 60 interfacing with cable select pins 42cs, two low data points (i.e. a 00) signature is returned to cable select pins 42cs. Accordingly, it can be seen that circuit 210 can be made to automatically identify the interface to which cable 60 is connected to, and can automatically adjust controls of I/O interface, of related circuit terminal 10 accordingly.

Additional features of the invention in an exemplary embodiment are understood with reference to the system architecture of Fig. 2b. Referring to interface-related features, RS 232 and 485 interfaces 254, 252 can share a common asynchronous receiver-transceiver as seen by DUART 278.

A switching function indicated in Fig. 2a by block 251 for switching the path between connector 42 and interfaces 254, and 253 can be provided by 232/485 level transceiver 272, which may be provided by a Linear Technology Model LTC 1387 Single 5U RS232/RS485 Multiprotocol Transceiver. Continuing with reference to Fig. 2b, IC chip 209 carrying CPU 212 can package certain interface circuitry such as USB interfacing circuits 252 and an IRDA interface 277. General I/O port 208 may provide output to indicator 287L and audio output 276 the latter, of which a programmer user may configure for operation with use of script programming or other programming, which will be described herein. In the exemplary embodiment, IC chip 209 is in communication with system BUS 207 which includes address and data buffer 274. In the exemplary embodiment system RAM 217 and system ROM 218 are provided. Additionally chip 209 including CPU 212 includes limited on-board RAM 217 and ROM 218. Terminal 10 in the embodiment of Fig. 2b is powered by a multiple voltage power system circuit 238 which distributes power to PCB 290. System 238 distributes power originating from, for example, a serially interfaced device, as indicated by USB box 252, an AC/DC power supply 239, e.g. a wall outlet plug-in power pack. and/or a rechargeable battery 268.

With reference to the transaction cycle flow diagram of Fig. 3a, an environment in which transaction terminal 10 may operate in accordance with the invention is described in greater detail.

Typically, transaction terminal 10 is disposed in a retail store klosk, or customer service desk. When a customer makes a transaction using a credit card or a debit card, an electronic benefits card (EBC) or customer loyalty card, a customer, at STEP 1, inserts a card into insert reader to read the card. A customer may, in addition, be prompted by

terminal 10 to enter PIN information into terminal 10, and may be prompted to write a signature on the terminal 10 so that terminal 10 can capture a signature.

About the time that a customer inserts a card into terminal 10, a sales associate, at STEP 2, enters the sales amount into POS network 300, to be described in more detail wherein, using e.g. a keypad 340K of cash register 340, or a bar code reader 342 or 263. In the alternative, the dollar amount can be entered into transaction terminal 10 at STEP 2. At STEP 3, transaction terminal 10 communicates a customer's card information data determined from a reading of the card and other transaction data to POS network 300. Transaction terminal 10 may also communicate PIN information of a customer to POS 300 as part of STEP 3. Also, a transaction terminal may communicate a captured signature to POS network 300 as part of STEP 3. More typically however, a signature may be captured by terminal 10 and transmitted to POS network 300 after authorization is complete as will be described herein. Signature data may be achieved for use in a signature recognition system by a retailer for recognition by a computer system of retailer POS Network 300 or as a third party, e.g. at a computer at 380. Transaction terminal 10 may also store signature data for later processing, which may be performed on a batch basis. Transaction terminal 10 may also archive other transaction data.

POS (Point-of Sale) Network 300, as is indicated in Fig. 3a, can take on a variety of forms. In any one of the layouts described, transaction terminal 10 can be considered part of POS network 300 once it is connected to POS network 300. In one simple form, as is indicated by Fig. 3b, POS Network 300 can comprise a modem 346 (e.g. cable or dial-up) or other communication device which provides communication debit network 320 or credit card network 322. Credit network 322

and debit network 320 may be the same network.

In another embodiment as indicated in Fig. 3c, POS network 300 and 300-2 may comprise a cash register 340. Cash registers are currently available in two popular forms. A PC POS system cash register 340 and 340-1, as shown in Fig. 3d, typically includes a personal computer housed in a standardly known PC housing 340PC and multiple interfacing or associated components including bar code reader 342, keyboard 340K, cash register drawer 340D, printer 340P, and monitors 340M. A dedicated POS Cash register, as shown in Fig. 3g includes the functionality of a PC and typically includes several of the above components (keyboard, monitor, printer, drawer) except that the components are housed in an integrated housing. Cash registers are equipped with communication interfaces e.g. dial-up or cable modem interfaces, USB interfaces, ethernet interfaces including wireless and nonwireless, which enable communication with external computer systems, including Terminal 10 and POS Network 300. In one embodiment, POS Network 300 comprises a cash register only and cash register 340 is adapted to communicate directly with a debit network 320 or credit card network 322.

Another embodiment of POS network 300 and 300-3 is shown in Fig. 3c. In the embodiment of Fig. 3c transaction terminal communicates with one cash register 340, while cash register 340 is one of several cash registers that is in communication with server 350, in an in-store local area network (LAN). In the embodiment of Fig. 3c in-store server 350 is in communication with debit network 320 and credit card network 322.

In yet another embodiment of POS network described with reference to Fig. 3e, POS Network 300 and 300-4 includes at least one computer system hub 360 which is under the control of a retailer yet located off-site with respect to transaction

terminal and other in-store devices such as cash registers or other transaction terminals and servers. Hub 360 may be in communication with, and may be adapted to monitor and control financial data transaction emanating from a plurality of in-store servers. Hub 360 may be controlled by a retailer that operates several stores at several different locations e.g. Store 1, Store 2, and Store 3. Further, there may be more than a layer of hubs. A retailer may operate a local hub which receives transactional data from each of several in-store servers located at several different stores located in a given municipality. Several of these local hubs, in turn, may transmit transactional data to a regional hub. Several regional hubs, may transmit transactional data to a centralized national hub. Several national hubs, in theory, can transmit transaction data to a single world-wide hub operated by a retailer having retail stores worldwide. It is seen that hubs and the layering of hubs provide a means for retailers to monitor transactions conducted throughout several retail stores. Hub 360 is often owned and operated by a retailer who owns or operates a retail store in which transaction Terminal 10 is located. However, Hub 360 may also be owned by a third party service provider, and the retail store owner may subscribe to a processing service provided by the third party. Such third-party operated hubs operated in the interest of a retailer shall herein be considered to be operated by a retailer. POS Network 300-4 of Fig. 3e is divided into zones. Zone 1 delineates the hardware components typically located in a first store, zone 2 delineates the network component typically located in a second store, zone 3, refers to components which are typically located at a third store, while zone x refers to components which are typically located off-site with respect to any store.

As indicated in the embodiment of Fig. 3e a POS Network

300 can also be considered to include various computer systems operated by parties other than a retailer or for example, a POS Network can include a Distribution Network 370. Distribution Network 370 refers to the computer systems operated by distribution service providers who receive transactional data from a retailer (e.g. from a computer system, a POS terminal such as terminal 10, a hub, a server, and a cash register) and evaluate the availability of several debit or credit card networks and route the data to one selected debit or credit card networks 320 or 322 based on an established criteria. Some transactions are processed without being routed through distribution networks and others are, normally dependent on the selection made by a retailer.

In a further aspect of POS Network 300, POS Network 300 can be in communication with another computer Network 380, which may be the Internet (World Wide Web). Connecting POS Network 300 to another Network 380 allows POS Network 300 to readily access information from a wide variety of computer databases, which information is pertinent to financial transactions. For example, by way of communication with Network 380, POS Network 380 can access such information as drive, license identification information, consumer credit rating information, consumer criminal record information, sales history information, consumer demographic data, and other consumer information. Aspects of the invention relating to access of information from Network 380 will be discussed in greater detail herein.

Continuing with reference to the transaction cycle flow diagram of Fig. 3a, at STEP 4, POS Network 300 routes transaction data either a debit network 320 or a credit card network 322 depending on the card type (debit or credit). Debit network 320 is a network of computer systems operated by a debit card agency. Credit card network 322, a network of

computer systems operated by a credit card supplier, such as Visa or MasterCard or a retailer issued credit card. After a transaction is approved by an Issuing Bank, Network 300 notifies POS Network 300 of such approval.

At STEP 5 debit card or credit card network 320 and 322 transmit the transaction data to a computer system (or a network of computer systems) operated by an Issuing Bank 330. Issuing Bank 330 provides a number of important functions in relation to the transaction processing cycle. Issuing bank (1) makes sure that a customer's account has sufficient funds; (2) charges a customer's account for a transaction; (3) charges a customer's account for any applicable fees in relation to the transaction, and distributes the funds to appropriate parties (e.g. Distribution Network operators); and (4) monitors for card holder fraud, (5) may automatically preliminarily authorize small dollar transactions, and (6) may preliminarily authorize transactions based on risk calculations which cannot be authorized because of technical problems (e.g. Network 322 is down); (7) capture and store a data record of the transaction.

At STEP 6, Issuing Bank 330 debits a customer's account, and may, as part of STEP 6, initiate action to obtain payment of the debt (if credit card transaction from a customer). For example, Issuing Bank 330 may send a bill to a customer's home mailing address notifying a customer of an amount of a debt. As part of STEP 6, Issuing Bank 330 may automatically notify a customer of a debit via email communication to a customer's email address, or may post a notice on the Issuing Bank's website so that the notice is read when a customer opens his account information from the Issuing Bank's website.

At STEP 7, POS Network 300 sends transaction data to a computer system a network of computer systems operated by an Acquiring Bank and Acquiring Bank 332 appropriately credits a

retailer's account by the amount of the transaction less any fees. Acquiring Bank (1) credits a retailer's account (2) charges the retailer any applicable fees and distributes these fees to appropriate entities involved in the transaction (e.g. Distribution network operators), (2) monitors for collection fraud, and (4) supplies information and customer service to a retailer, in part through communication with POS Network 300. Typically, STEP 7 is a batch process performed e.g. after business hours, whereas STEPS 1 through 6 described herein are all performed automatically after a transaction is initiated, within seconds of one another (except the nonelectronic mailing step described as part of STEP 6). In some instances STEP 7, is carried out with manual data entry and human observation of financial data records.

Some further aspects of possible transactions involving Terminal 10 can be understood with reference to the following examples, EXAMPLE I and EXAMPLE II, wherein the term "host" in Example I and Example II is used to refer to a computer system or network of computer systems interposed between a cash register and a debit/credit networks 320 and 322 as described above with reference to Fig. 3a., e.g. a "server," or a "hub," or a network comprising a plurality of servers and/or hubs.

EXAMPLE I (Debit Transaction and Authorization)

The purchaser may initiate the transaction or be prompted by the POS device. Electronic Benefits Transfer (EBT) using magnetic stripe cards or smart cards is similar to a debit transaction. Rules and exact procedures varies by State. Note: "Off-line debit" processes as if it were a credit card transaction. Ordering of steps:

(A) Associate 312 initiates a new sale and begins scanning items;
(B) Purchaser 310 selects their payment option = debit;
(C) Terminal 10 saves customer selection = debit;
(D) Purchaser 310 inserts their card on the terminal

MSR/SCR;

(E) Terminal 10 stores the credit card track data;

(F) Terminal 10 request PIN;

(G) Purchase 310 enters PIN;

(H) Terminal 10 encrypts PIN block and stores the result;

(I) Terminal 10 waits for POS 340 terminal request;

(J) Associate 312 completes the sale;

(K) POS 340 sends sale total to Terminal 10, waits for reply;

(L) Terminal 10 displays total and prompts the purchase for "cash back";

(M) Purchaser 310 responds to cash back prompt, "yes" + amount or "no"; Terminal 10 requests confirmation and displays new total;

(N) Terminal 10 replies to POS 340 with track data, PIN block and "debit" flag;

(O) POS 340 sends the amount(s), card data, PIN block, terminal ID, etc. to host 300;

(P) Host 300 adds merchant data and forwards to authorization Network 320;

(Q) Network 320 translates PIN block encryption to Zone key (Each network switch and processor translates the incoming PIN block to the encryption algorithm and key of the next zone);

(R) Network 320 examines card Bank ID Number (BIN) and routes to issuing bank;

(S) Issuer 330 checks account balance, account status, and fraud data;

(T) Issuer 330 verifies PIN;

(U) Issuer 330 replies "yes" or "no" for authorization or an error code;

(V) Network 320 sends issuer response to retailer host;

(W) Host 300 routes the issuer/network response to a POS terminal 340;

(X) POS 340 notifies associate of issuer response;

(Y) POS 340 sends message to Terminal 10 authorized or declined.

If authorized, the transaction is complete from the Terminal 10 point of view.

Note: All PIN-based payments are encrypted. Responses are not encrypted or secure.

{End of Example I}

EXAMPLE II (Credit Transaction and Authorization)

The following describes typical credit card transaction flow

in U.S. networks for transactions initiated on a connected POS terminal.

The purchaser may initiate the transaction or be prompted by the POS device.

(A) Associate 312 initiates a new sale and begins scanning items;
(B) Purchaser 310 selects their payment option = credit;
(C) Terminal 10 saves customer selection = credit;
(D) Purchaser 310 inserts their card on the terminal MSR/SCR;
(E) Terminal 10 stores the credit card track data, waits for POS terminal request;
(F) Associate 312 completes the sale;
(G) POS 340 sends a message to the Terminal 10 = "send data";
(H) Terminal 10 replies to POS with track data and "credit" flag;
(I) POS 340 sends transaction amount, card data, terminal ID, etc. to host along with merchant data;
(J) Host 300 adds merchant data and forwards to authorization to network;
(K) Network 320 examines card Bank ID Number (BIN) and routes to issuer;
(L) Issuer 330 checks account balance and fraud data;
(M) Issuer 330 replies "yes" or "no" for authorization or an error code;
(N) Network 320 sends issuer response to retailer host;
(O) Host 300 routes the issuer/network response to the POS terminal;
(P) POS 340 notifies associate of issuer response;
(Q) POS 340 sends message to Terminal 10, authorized or declined.
(R) Purchaser 310 signs signature on touch screen 320;
(S) Signature saved at terminal 10 and/or transmitted to POS for further processing (e.g. signature recognition).
If authorized, the transaction is complete from the Terminal 10 point of view.

Note: In the United States, credit transactions are not encrypted. Responses are not encrypted or secure. Credit transactions that are processed in Canada are encrypted and use MACing for data integrity.

{End of Example II}

Referring to further aspects of the invention, housing 11

of terminal 10 includes a number of important features which will now be described in greater detail. Housing includes a top 11t, a bottom 11b, a first side 11s, a second side 11s, a back end 11rr, and a front 11f. As best seen in Fig. 1e, top 11t which being substantially flat is angled downward slightly from back 11rr housing to front 11f. Because touch screen 20 is disposed substantially flush with top 11t of housing 11 the angling of top 11r enables a user to more readily observe indicia of housing when terminal 10 is disposed on a flat surface, e.g. a counter top. Housing 11 further includes a head 11h including housing top 11t and a base 11bs including bottom 11b.

Referring to aspects of bottom of housing 11b with reference to Figs. 1j and 1k, bottom 11b of housing 11 includes at least three and preferably four or five feet 15, typically comprised of rubber adhesively attached material which stabilizes housing 11 on a counter top. The at least three feet 15 define a plane P_B on which housing 11 may rest. Housing 11 may further include detachable riser 11r also including at least three and preferably five feet 15-r. Detachable riser 11r operates to increase the height of transaction terminal 10 where a height increase makes use of terminal 10 easier. As best seen in Fig. 1e, head 11h of housing 11 extends forwardly from base 11bs to define a lip 11L, and mold support section 11sp of housing 11 which supports hybrid reader 240 is defined in the lip 11L of housing 11. It is seen that if housing 11 is fixed mounted on an edge of a table top so that lip 11L extends outwardly from the edge, the riser 11r may be unnecessary since a user's hand will not encounter substantial interference from counter top when inserting a card 90 into reader 240. However, if transaction terminal 10 is to be mounted or rested away from an edge of a counter top, attachment of riser 11r to housing

main body 11mb will improve the accessability of reader 240 to a user, and will prevent the table top from substantially interfering with a user's hand when a user inserts a card 90 into insert reader 240. Attachment of riser 11r will also benefit access to a reader by a user's hand where terminal base 11bs is mounted flush on a vertical wall, beam or post. Thus, it is seen that attachment of riser 11r improves the accessability of reader 240 under certain mounting or placement conditions while attachment of riser 11r reduces the size of terminal 10 under other mounting or placement conditions. The "feet" of terminal as will be referred to herein shall refer to feet 15r of integrated housing bottom 11b when no riser is attached to housing main body 11nb, and to the to feet 15-r of riser 11r when riser 11r is attached to main body 11nb. Riser 11r may be made detachably attachable to housing main body 11nb by way of a pin and key-slot arrangement as shown in Figs. 1j and 1k. Riser 11r may include headed pins (not shown) which are fitted into hole sections 17h of key slots 17 formed on bottom, and the riser 11r may be detachably engaged on body 11mb by sliding the headed pins into slot section 17s of key slots 17. As indicated in the embodiment of Fig. 1r, riser 11r may also be of a type that is bolted into integral bottom 11b of terminal by driving bolts through bolt holes 23 of riser 11r. Other fastening agers for detachably attaching riser 11r to main body 11mb can of course be used, such as clips and adhesives (e.g double sided adhesive pads).

As seen in Figs. 1g and 1j, key slots 17 and 17r are useful in detachably mounting terminal 10 in a mounted mode of operation to mounting (e.g walls, posts, retailer mounting apparatuses, horizontal surfaces) members having pins (not shown) for receiving key slots 17 and 17-b, so that at any time terminal 10 can be detached and used on a horizontal

surface such as a countertop in an unmounted mode of operation.

As shown in Fig. 1f risers need not be made of a uniform height. Wedge shaped riser 11r-w, for example, is useful in certain applications. Wedge riser 11r-w may be detachably attached to terminal main body 11mb and then terminal 10 including main body 11mb and wedge riser 11r-w may be mounted to a vertical member such as a wall, a vertical beam, or a post. The mounting method results in plane P_R of reader slot 245, and plane P_S of screen 20 being moved to a position that is closer to the parallel position with respect to the horizontal plane. Many users will find insert reader 240 easier to use if it is oriented in a plane tilted forwardly toward the horizontal plane relative to the vertical plane.

Dimensional information relating to terminal 10 in one exemplary preferred embodiment is summarized in Figs. 1r, 1s, 1t and 1u wherein dimensional information is given in inches. In an exemplary embodiment as seen in Fig. 1u, feed path slot 245 is positioned about 1 inch off ground level and 2 inches off ground level with riser 11r attached, which in the exemplary embodiment of Fig. 1r includes a height of about 1 inch. The inventors found that with such a height range of slot 245, preferred angles for angling feed slot plane, P_f, are between about 2° and 12° with a most preferred angle being about 7°. The inventors found that at angles greater than this range, at the height range of between about 1 and 2 inches, card 90 became difficult to insert into reader 240 though the difficulty can be alleviated by mounting terminal on an edge of a counter or by increasing its height. At angles less than the above range, the benefits of angling, discussed fully herein, though substantial, were determined to be outweighed by the design and assembly costs attendant to such angling. Because the options for angling of plane P_s are

not limited by card insertion concerns, it is seen that plane P_s can normally be angled at a steeper angle than plane P_f. However with such inconsistent angling, the benefits yielded by essentially coplanar positioning of plane P_f and plane P_s to be described more fully herein would not be yielded.

Additional advantages of the positioning of slot 245 according to the invention are described with reference to Figs. 7a and 7bm wherein 7a is a functional diagram of slot 245 disposed parallel to horizontal plane PH, Fig. 7b is a functional diagram of slot 245 disposed at a slight angle with respect to horizontal plane P_H, and arrows 710 and 711 indicate the general direction of card 90 when it is removed from feed slot 245. It is seen by observation of either embodiment, the positioning of slot 245 substantially in horizontal plane P_H yields the possibility of a "fulcrum and brooming effect" as will be described herein

A fulcrum and brooming effect is yielded when card 90 is pivoted about a fulcrum 712 defined by slot top edge 712. When card 90 is pivoted about fulcrum 712 distal end 90d of card 90 imparts a force against bottom 345b of slot 3455. Therefore, when card 90 is pulled out card 90 will operate as a broom to sweep debris, moisture, particulate matter out of slot 90.

It is seen further with reference to Fig. 7b that the fulcrum and brooming effect will be enhanced when slot 345 is positioned at a slightly downward angle with respect to the horizontal plane. If terminal 10 is positioned below a user's elbow level, as it often will, user's natural tendency will be to be to pull card up and out as indicated by arrow 711 or possibly, straight out horizontally as indicated by arrow 710. The fulcrum and brooming effect is yielded in both embodiments when a user pulls card out and up as indicated by arrow 711. In addition, it is seen from Fig. 7b that the

fulcrum and brooming effect can be yielded with slot 345 disposed at a slight downward angle even when card 90 is pulled straight out in the horizontal direction indicated by arrow 710. Further, disposing slot 345 at an angle increases the force supplied by card end 90d on slot bottom 345b when the fulcrum effect is present to enhance the cleaning action of the card. Still further, the brooming effect cleaning action of card 90 in the embodiment of Fig. 7b is multiplied by gravitational pull forces provided by the angling of feed slot 345.

An important aspect of the invention is the positioning of insert hybrid slot reader 240 in terminal 10 in relation to other components of terminal 10. Insert reader 240 is disposed in the front of terminal 10 and is accessible from the front of terminal 10. Accordingly, when a card is inserted reader 240, a user's view of screen 240 is not obscured as in the case of the prior art transaction terminal 700 of Fig. 7 having rear disposed, top opening-swipe style reader 710 and a display 720. Reader 240 is also disposed in lip 11L of terminal head 11h which extends forwardly from base 11bs of terminal 10. Therefore, a space s is defined by reader housing 11 as indicated by Fig. 11h for accommodating a person's hand while a card is inserted into reader 240 of terminal 10. Still further insert reader 240 is disposed so that a plane P of feed slot P_f of insert reader 240 is substantially parallel to a plane P_s of screen P_s. Accordingly, indicia of screen 20 and indicia of card 90 are easily viewed at the same time from the single vantage point of a user. In the embodiment shown in Fig. 1i it is seen that a plane P_f of feed slot P_f is substantially parallel to plane P_{b-r} of feet 15-r, and plane P_s of screen 20, but that slot 245 is closer to a parallel relationship with touch screen plane P_s than it is to base plane P_{b-r} (i.e. slot plane P_f is essentially

parallel to screen plane P_s, and slightly angled with respect to feet, or base plane P_{b-r}). It will be seen that slot plane P_f could also be disposed in terminal 10 to be essentially parallel with base or feet plane P_{b-r} and slightly angled with respect to screen plane P_f, or slightly angled with respect to both base plane P_{b-r} and screen plane P_s. It is preferred in the embodiment shown to dispose slot plane P_f essentially parallel with screen plane P_s so as to discourage the build up moisture of dust, debris, and other particulated matter (angling slot downward encourages a percentage of particulate to be forced out of slot 345 by gravity and the fulcrum and grooming effect described herein) and to reduce the number of positions at which specular reflections on either card or screen are observed. Whatever the orientation of slot plane P_f in relation to screen plane P_s and base plane P_{b-r}, P_b it is important, in the embodiment shown in Figs. 1a-1e that screen plane P_s be slightly angled with respect to base plane P_{b-r}, and P_b. Configuring terminal 10 so that screen P_s is angled with respect to base plane P_{b-r}, and P_b assures that screen 20 is readily viewed when base 11bs is situated or mounted on a horizontal counter top. Still further, referring to mounting features of insert reader 240 insert reader 240 is disposed proximate right side 11s of terminal 10 in lip 11s so that reader 240 is readily accessible by a user's right hand, allowing a user to readily center his head toward center of screen 20 while inserting card 90 into reader 240. The positioning of insert reader 240 as shown in addition renders reader 240 resistant to degradation resulting from environmental effects. It is seen that in prior art terminal 900 having slide or "swipe" reader 910 opening toward a top of terminal 90, dust and debris, which are prevalent in many retail environments, can readily enter top-opening slot 910 and become trapped therein to negatively impact the

functioning of terminal 900 reducing the product life of terminal 900. The orientation of insert reader 240 substantially parallel to the horizontal plane results in a reduction in the volume of moisture (as may be caused by cleaning) dust and debris and other a particulate matter from the retail environment which enter reader 240. As indicated previously, angling slot 245 downward with respect the horizontal plane further reduces particulate and moisture build-up in slot 245 because such angling further reduces the amount of particulate that can enter slot 245 and encourages a percentage of particulate and moisture that does enter slot 245 to be forced out of slot 245 by gravity.

As best seen Figs. 6a-6d, hybrid reader unit 240 may comprise a packaged modular form factor. Reader unit 340 may be packaged in a form that does not include SAMS IC chips 610, as indicated by Figs. 6a and 6b, and may, in the alternative be packaged in a form that does include SAMS chips 610, as best seen in Figs. 6c and 6d. SAMS (Security Access Module System) is a system in place in some transaction cycles for support mainly of customer loyalty card applications and cash card applications. SAMS IC chips 610 are necessary for support of SAMS. As part of SAMS, SAMS IC chips 610 must, from time to time be removed from devices in which they are installed and replaced. In accordance with the invention as best seen in Figs. Ij and Ik, transaction terminal housing 11 may include a SAM access door 612 for allowing access to SAM IC chips 610 without requiring disassembly of housing making body 11MB (which all be discussed would trip a security circuit). Housing 11 as seen in Figs. Ij and Ik may include SAM access door 610 detachably attachable or pivotally attached to housing bottom 11b.

Referring to further aspects of terminal 10 relating to housing 11, terminal 10 further includes stylus holder

apparatus 70 which is described in detail with reference to Figs. 1-3 and 5c-5f. Holder apparatus 70 is a one-piece stylus mounting apparatus, including both a well 72 for holding a stylus 74 and a connection device 73 for connecting a systems cord. By contrast, in prior art transaction terminal 700 shown in Fig. 7 stylus 730 is held in holder 740 while stylus cord 750 is connected to prior art terminal on a connection point 760 away from holder apparatus 740. Providing a one-piece stylus holder apparatus 70 which both includes a holder which holds pen stylus 74 and which includes a proximately disposed connection device 73 for cord 75 greatly is particularly advantageous when one-piece holder apparatus 70 is adapted to be detachable with respect to housing 11. It is seen, if holder e.g. 72 and connection device 73 are provided at different spaced-apart locations on housing 11 as in terminal 900, positioning of holder 72 at a position away from terminal 10 (such as mounting it on a wall, a counter top, a beam, and a cash register) would be disadvantageous because the cord 75 would assume a stretched-out state. If cord 75 is in a stretched out state, entry of a signature by a user is rendered difficult. Providing a holder apparatus 70 which includes both cord connection device 73 and a proximally located pen holder 72 yield a significant advantage if holder apparatus 70 is made non-integral and selectively attachable with respect to housing 11. Where holder apparatus 70 is adapted to be nonintegral and selectively attachable with respect to housing 11 holder apparatus 70 can be moved into a variety of positions (e.g. mounted to a wall, counter top, cash register, etc.) in the general area of terminal 10, and in anyone of those variety of positions, cord 75, connected to connection device 73 remains in an untensioned state when pen stylus 74 is held by holder 72. The detachability of holder apparatus 70 allows apparatus

70 to be moved if there is interference with cord 75 by an object in processing with terminal 10.

In the present invention, holder apparatus 70 may be made selectively attachable to housing 11 with use of a double-stick adhesive pad (referred to as double stick tape) of one of the many types available from 3M, for example, or with other types of fasteners. In Fig. 5e it is seen that holder apparatus 70 includes broad surface 76 for receiving double-stick tape (not shown). When double-stick tape is applied to holder apparatus 70, holder apparatus 70 may be tape mounted to any one of a variety of positions selectable by a user including positions on housing 11 and away from housing 11 (e.g. wall, cash register, etc). Because cord connector 73 is integral with holder apparatus 70 and proximally located with well 72, cord 75 of stylus 74 will be untensioned when held by holder 72 wherever holder apparatus 70 is mounted. Holder apparatus 70 could also be selectively mounted with e.g. other adhesives or a mechanical fastener such as a screw, bolt, or key slot faster such as fastener 17 as shown in Fig. 1j. Holder apparatus 70 including connection device 73 may include another holder member for holding stylus 74 in place of well-style holder. For example, holder apparatus 70 can include a groove or slot (not shown) which holds a pen stylus by friction forces. Connection device 73 of holder apparatus 70 can take on difference to forms as well. In the embodiment of Fig. 5f connection device 73 is provided by a set screw bore which receives a set-screw 78. Ring eyelet 77 of cord 75 is disposed about set screw 78 and set screw 78 is threaded into threaded bore 73 to secure eyelet 77 against holder apparatus 70. Connection device 73 could also comprise, for just one example, a hole formed on holder apparatus 70 which accommodates cord 75, wherein cord 75 is prevented from slipping out of the hole by means of a knot formed in the cord

having a diameter larger than the hole diameter.

Referring to further aspects of stylus 74, a connecting arrangement for connecting stylus-end 79 of cord 75 to cord-end 80 of stylus 74 is described in detail with reference to Fig. 5a. In one embodiment for connecting cord 75 to pen stylus 74, distal end 80 of pen stylus 74 is made to include a stepped bore hole 82 and stylus end 79 of cord 74 is made to include an enlarged cord end. More specifically, stepped bore hole is made to include at least two different diameters, d1 and d2, to define an enlarged bore section 83 and a narrowed bore section 84. Cord 75 is configured complementarily with stepped bore 82 to have a distal end 79 of an enlarged diameter that is greater than the diameter, d_1, of the narrowed bore section 84, but less than the diameter, d_2, of the enlarged bore section so that enlarged distal end 79 is retained by narrowed bore section 84. Cords major body 85 should have a diameter sufficiently less than narrowed section 84 of stepped bore 82 so as to allow free rotation of cord 75 within narrowed section 84. Configuring cord 75 to have an enlarged section 79 which is accommodated by an enlarged section 83 of bore hole 82 formed in stylus and retained by a narrowed section 84 of the bore hole 82 that has a diameter sufficient to allow free rotation of the cord major body 85 allows cord 75 to rotate freely within pen stylus 74, and thereby prevents against the twisting of "kinking up" of cord 75. Stepped bore hole 82 may further include a third bore section 87 formed outwardly with respect to narrowed bore section 87. Third bore section 87 preferably includes a diameter slightly larger than narrowed bore section 84. It will be seen that third bore section 87 operates to alleviate substantial tension forces and stresses which would be supplied by narrowed bore section 84 on cord 75 at distal end 82 of narrowed bore section 84 in the absence of third section

87. Cord 75 can be configured to have an enlarged cord section 79 by means of e.g. a cap, or a crimped-on metallic member as is shown in Fig. 5b.

In a still further aspect of housing 11, the colors and/or patterns exhibited by the exterior of housing 11 can adapted to aid a user in orienting card 90 in relation to slot 345. As best seen in the top view of Fig. 1c housing top 11t preferable includes stripe 730 which divides housing into a first reader zone 732 and a second nonreader zone 734. Stripe 730 encourages a user to move a card toward reader zone 732 of terminal 10 when moving card 90 in proximity with terminal 10. Further in accordance with the invention, reader zone 732 in one embodiment is preferably manufactured to exhibit a different color than nonreader zone 734 so that reader zone 732 further stands out in relation to nonreader zone 734 to further encourage a user to move a card toward reader zone 732 as opposed to nonreader zone 734 when moving a card toward terminal 10. Zone 732 may made to exhibit a darker color than zone 734.

Importantly, housing 11 when manufactured to exhibit multiple colors should be made to exhibit different colors without substantially weakening the structural support and protection provided by housing 11. Housing 11, which may comprise a polycarbonate ABS blend, can be made to exhibit different colors as between zone 732 and zone 734 without substantial degradation of containment advantages provided by housing 11 by utilization of a two-shot molding process during the manufacture of housing upper section 11up, wherein a first shot of the two-shot molding process defined the color of zone 732 and a second shot of the two part molding process defined the color of zone 734.

In yet another aspect of the invention, housing 11 can be made to exhibit colors or patterns in accordance with the

colors and/or patterns for terminal that are desired by the buyer-retailer of terminal 10. The inventors discovered that the most desirable colors and patterns for housing 11 vary greatly between different retailers. Some retailers may desire bright colors for terminal 10 in an effort to attract attention to terminal 10. Other retailers may desire subtle colors for terminal 10 in an effort to reduce psychological stresses which are sometimes associated with the expenditure of personal funds. Still other retailers may desire pattern and colors for terminal 10 that are in accordance with its company trademarks and or advertising campaigns. Other retailers may desire that terminal 10 carry advertising of a third party business which will subsidize at least in part the cost of terminal 10.

Accordingly, the inventors have adopted a business method for marketing and supplying terminal 10 that is explained with reference to the business model diagram of Fig. 7c. At step 1, a supplier 750 (who may be a manufacturer of terminal 10) informs a retailer and buyer of terminal 10 that terminal 10 can be made to exhibit customizable patterns and/or colors. At step 1, supplier may advertise to retailer that a limited number or unlimited number of design/color options are available to retailer. Step 1 may be accomplished through information published on an internet website of a supplier 750. At step 2, retailer 752 communicates his pattern and/or color request to supplier 750 such as though a telephone call or by a request entered in the supplier's website. At step 3, a supplier 750 relays the request of the retailer including address information to a graphics forming business entity 754 that specializes in forming graphics on Ruggedized material. The graphics forming business entity may be owned by supplier 750. The graphics forming business entity may be an organization such as Immersion Graphics Corp. who specialize

in an immersion graphic formation process. The graphics forming business entity may have a stock supply of terminal 10 or else terminals 10 may be shipped from supplier 750 to entity 754 on an as needed business. At step 4, the graphics forming business entity 754 forms a graphic on a built terminal 10 in accordance with the method which it specializes in. At step 5, graphic forming business entity 754 ships the graphic-carrying terminal 10 to retailer 752 in accordance with the information previously received from supplier 750 regarding the retailer at step 3. Step 5 may be executed by shipping the finished product back to supplier 750 who then routes the product to retailer 752.

Referring to further aspects of the invention, terminal 10 may be equipped with a variety of security features, which may take on a variety of forms. Referring to a first security feature, housing 11 is adapted so that if an unscrupulous party attempts to break into housing 11 to steal secure information from a storage device of terminal 10, the secure electronically stored information is automatically destroyed. Referring again to electrical block diagram 2a of Fig. 2a, terminal 10 includes a security circuit block 220, an embodiment of which is shown in greater detail in Fig. 2c. As shown in Fig. 2c security circuit block 220 may include in one embodiment, an integrated circuit chip 221 having volatile memory. In the embodiment shown, chip 221 has both a volatile RAM 222, a ROM 223, and includes a CPU 224. Secure chip 221 preferably includes submicron electrical connections rendering it extremely difficult to read information from chip 221 using electrical probes.

Transaction terminal 10 is adapted so that certain information previously designated as secure information is stored in a designated IC chip. Such information may include, for example, encryption keys or other information which may be

designated as secure such as card identification numbers, signature information, fingerprint information, and retinal signature information, decoded-out message data decoded from e.g. an optical or RF card reader. In accordance with applicable banking standards (ANSI ISO), PIN information, when entered into a POS device such as transaction terminal 10 should be encrypted at terminal 10, as will be explained. From time-to-time, encryption keys stored in terminal 10 may be updated and replaced with new encryption keys. As will be described in further detail herein, transaction terminal 10 is adapted so that when a user enters PIN information in response to a prompt for PIN information displayed by terminal 10, an encryption algorithm stored in ROM 223 of secure chip 221 is called for execution by IC chip CPU 224 to encrypt the pin information in accordance with an encryption key stored in RAM 222. Encryption keys may be stored in other, mechanically and logically secure, preferably erasable, storage locations.

Encryption keys which terminal 10 may use for PIN encryption typically comprise one of two types: "master session" and DUKPT. Master session keys are used by a symmetrical encryption algorithm. The Data Encryption Standard (DES) is the most common form of master session keys. Under a master-session scheme, terminal 10 has a strong "master" key and a second "session" key. Typical implementations use a weaker session key. The session key is used to encrypt PIN blocks. The master key is used to secure replacement session keys. Terminal and the first computer (host) of POS Network 300 that receives and processes the encrypted PIN block must have the same key. POS Network 300, comprised of many "nodes" or computer systems connected by various communications links, translates the PIN from the key used by the sending device (terminal, host, etc.) to the encryption key and scheme used by the next node in the

transmission chain. This repeats until the encrypted PIN block arrives at Issuing Bank 333. Accordingly, "security zones" are created which increase the difficulty of an unscrupulous party compromising the system. It also allows each zone to trust only the devices with which it directly communicates. It also greatly simplifies distribution of the symmetric keys. A given node must only deal with two other nodes rather than every node in the chain. Debit card Issuing Bank 333 does not convert the PIN block to clear data. Issuing Bank 330 submits the encrypted PIN block to a security device commonly called a Network Security Processor (NSP). The NSP verifies the PIN validity and returns a "yes" or "no" response. That response is utilized by issuing bank 330 for verifying the validity of the PIN entered on transaction terminal 10.

Derived Unique Key Per Transaction (DUKPT) keys and encryption scheme is common in POS terminals and PIN pads installed since 1997. The advantage of DUKPT and other similar schemes is that each PIN block encryption uses a new ("unique") key whereas the master session encryption uses the same key for all transactions. In DUKPT PIN systems, over 1 million keys can be generated from an initial base key. The "T" in DUKPT can also mean "terminal" since the terminal ID is used to generate the key set, a given base key can create many unique key sets. DUKPT PIN encryption keys are unique and no key can be computed from any other key. So if a given transaction key is compromised, no other transactions are at risk. The base key is not stored in the terminal. The current method of PIN encryption using DUKPT is similar to the master session encryption method described above. Additional data is used and the key is applied to the PIN block only for the current transaction. The node security zones are substantially identical to those described above with

reference to the master session described above. In many systems, the terminal's DUKPT PIN block is translated to a master session PIN block at the first intercept computer system which may be e.g. a POS Network computer system of a retailer, or a computer system third party network provider. The conversion allows the simpler master session to be used for relatively secure host/server point to point communications. The computer centers are physically more secure than distributed transaction terminals. Issuing Bank 330 then processes the authentication according to the master session method described above.

With master session keys, all PIN blocks encrypted with a given key can be decrypted if the key is compromised. Since the master session key is stored in a relatively less secure terminal and distributed in publicly accessible locations, the risk of attack is greater. To reduce the risk, most implementations allow for a periodic key exchange where a host system generates a random key value, encrypts it under a strong exchange key and sends it through POS Network 300 to the terminal 10. All nodes between the originator and the terminal must be able to handle the key exchange. When the new session key arrives at terminal 10, terminal decrypts the new session key from the master key (which also resides in the terminal) uses the key for subsequent PIN block encryptions. DUKPT keys normally do not have to be replaced unless the entire key set is exhausted or the well protected base key is compromised. Further, a data integrating encryption algorithm (e.g. MAC) may be utilized by terminal 10.

With further reference to a tamper-detection security feature of the invention, the selection of an IC chip including integrated RAM, ROM and a CPU, wherein encryption keys are stored in volatile RAM 222, an encryption algorithm is stored in ROM 223, and the algorithm is executed by

integrated CPU 224, yields an important benefit. If the CPU that executed the encryption algorithm were stored on an IC chip separate from the chip including volatile RAM 222, then an unscrupulous party may attempt to intercept the unencrypted PIN data, with use of probes, while it is being retrieved by the CPU from its storage location in RAM. The arrangement above protects against the above potential security breach. An unscrupulous party could not readily, if at all, contact probes onto circuit tracings of packaged secure IC chip 221 comprising RAM 222 and ROM 223.

As indicated in Fig. 2c, IC chip 221 having volatile RAM 222 and ROM 223 is powered by a battery 225 so that information stored in chip 221 is destroyed by disconnecting battery 225 from chip 221. Battery 225 may be a 1400-1800 ma hour battery. Chip 221 may be provided, for example, by a Hitachi H8S/2318 F-2TAT HD64FZ318 IC chip.

Description of a terminal break-in theft prevention scheme is made in further detail with reference to the block diagrams Fig. 2c and 2d, Figs. 4b-4c (showing partial internal perspective views terminal 10, and particularly the interface between housing 11 and main circuit board 290 of terminal 10) and Fig. 4a showing an assembly diagram for terminal 10. Main circuit board 290 carries the majority of electrical circuit components of terminal 10. Main circuit board 290 carries all or essentially all of the electrical components described with reference to Figs. 2a-2c herein including control circuit 210 and secure chip IC 221.

Referring to the assembly diagram Fig. 4a transaction terminal housing main body 11mb includes an upper mold 11up which is interfaced to lower mold 111w during the assembly of terminal 10. As best seen in Fig. 4b upper mold 11up includes four PCB contacting struts 410 each comprising a bolt-retaining hole 412 for accommodating a bolt 416 or screw.

Struts 410 are configured to be of such a length so that struts 410 impart a compression securing force to PCB 290 when upper mold 11up and lower mold 111w of transition terminal 10 are connected together. With further reference to Fig. 4a, PCB 290 includes four open contact washers 292 integrated into circuit board 290. As best seen in the exploded view of Fig. 4a open contact washers 292 each comprise an insulation space 292 so that an electrical connection between first conductive section 292c1 of open contact washer 292 and second conductive contact 292c2 of washer 292 can be made by applying a conductive bridge between the conductive contacts. PCB 290 and upper mold 11up are complementary configured so that each of the open contact washers 292 opposes one of the struts 410. When upper mold 11up is applied to lower mold 111w (on which PCB 290 is previously mounted) struts 410 impart pressure on PCB 290 at each of the open contact washers 292. In accordance with the invention, contact security washers 295 are interposed between struts 410 an open contact washers 292 at each of the four contact points at the time that upper mold 11up is applied to lower mold 111w. Contact security washers 292 serve as conductive bridges between the conductive sections of each of the open contact washers 292. Accordingly, it can be seen that if any attempt is made to remove any part of upper mold 11up from lower mold 111w electrical contact between conductive sections 292c1 and 292c2 of at least one of the open contact washers 292 will almost certainly be destroyed. To increase the likelihood that electrical contact between conductive sections of at least one of the open contact washers 292 will be destroyed by a tampering attempt, contact washers 295 can be fixedly secured to the distal ends 410e of struts 410, e.g. by an adhesive bonding material. Securing washers 292 to struts 410 assures that contact between conductive sections of washers 292 will

be destroyed if upper section 11up is lifted from lower section 11lw. The four open contact washers are disposed at spaced apart positions about circuit board 290. Such positioning increases the likelihood that electrical contact between conductive sections of at least one of the open contact washers will be destroyed by an attempt to remove only a part of upper mold 11up from terminal 10. Terminal 10 is preferably adapted to that each of the bolts 416 engages a threaded bore hole when driven into terminal 410. Threaded bore holes engaging bolts 416 may be formed on either of both of circuit board 210 and lower mold 11lw.

As is indicated by the electrical schematic diagram of Fig. 2c open contact washers 292 may be serially connected in a circuit powered by security circuit battery 225 (e.g. by circuit traces etched on PCB 290) and contact sensing circuit 226 may be disposed in communication with open contact washers 292 to sense whether electrical contact between conductive sections 292c1 and 292c2 of one of the washers is destroyed. If contact between conductive sections of any one of the open contact washers 292 is destroyed, sensing circuit 226 generates a tamper signal. Terminal 10 may be configured so that if terminal in a powered-down mode a tamper signal generated by sensing circuit 226 operates to disconnect secure IC chip 221 from battery 225 as is indicated by switch 227. Terminal 10 may also be configured so that generation of a tamper signal when terminal is in a powered-up mode (wherein secure IC chip 221 is powered by an external power source) results in an erasure instruction being generated that causes the secure (e.g. encryption information) of chip 221 to be erased. The tamper signal causing the erasure instruction to be generated may be communicated from sensing circuit 226 to e.g. control circuit 210 or to secure chip IC 221 as indicated by dashed-in contact 228.

Security circuit block 220 may also be configured so that IC chip 221 is erased by disconnecting power therefrom when there is a security breach whether terminal 10 is in a powered-down mode or powered-up mode. In the embodiment if Fig. 2d, DC supply, described with reference to Fig. 2b and security battery 225 are both tied to switch 229, (which may comprise a simple diode circuit) that is responsive to losses in DC supply power 238 so that security battery 225 power chip 221 only when there is a loss of supply power. It is seen that in the circuit of Fig. 2d, that the power supply to IC chip 15 is disconnected to erase information in RAM 222 when there is a security breach resulting in one or more contacts 292 opening whether terminal is powered up-or powered-down mode. Circuit 220 in Fig. 2d includes an isolation circuit 293. Isolation circuit 293, which may be for example, a TISN74CBTLV3126 FET bus switch, isolates circuit 210 from circuit 221. Isolation circuit 293 prevents power from chip 221 from powering circuit 210 when there is a loss of power in circuit 210 and prevents circuit 210 from powering circuit 221 when there is a loss of power in circuit 221. Isolator 293 may have a data pass mode (allowing data flow) and a data isolation mode (isolating the circuit). The data pass and isolation modes of circuit 293 may be made responsive to the voltages produced by meter 294 which senses the voltage input to chip 221 and meter 296 which senses voltage input to control circuit 210.

Referring to further aspects of the invention and relating to the security feature just described, transaction terminal 10 in the assembly view shown in Figs. 4a and 4b may include lower and upper cover panels 21 and 22 some features of which are described in U.S. Application Serial No. 09/750,479 filed December 28, 2000 assigned to the assignee of

Lower cover panel 21 including open window 21w surrounds overlay 230 and covers electrical lead lines carrying data from overlay 230. Lower over panel 21 is bonded to upper section 11up to create a moisture and dirt-tight seal there between, as well as physically protecting the lead lines. Second upper cover panel 22 is placed over lower panel 21. Upper panel 22 includes a frame 22f and a light transmissive protective window 22w mounted in frame 22f. When upper panel 22 is disposed on lower panel 21 protective window 22 is in close proximity with overlay 230 so that a signature written on window 22w will be recorded by overlay 230. The lower surface of upper panel 22 contains an adhesive whereby the upper cover panel can be easily removed when window 22w becomes worn or damaged. A warning message 21m is printed on lower panel 21 which is clearly discernable when the upper cover panel is removed, warning the user not to write upon touch screen 20 until the upper panel is replaced.

In a further aspect of a panel system according to the invention, upper section 11up and panels 21 and 22 are complementarily formed so that bore holes 419h and the bolts or screws 416 which they accommodate are completely hidden from view when panels 21 and 22 are attached to housing 11. In the embodiment of Fig. 4a, it is seen that bolts or screws 416 which operate to secure upper section 11up to lower section 11lw are accommodated by bolt holes and are formed in housing 11 in such a position that both fasteners 416 and holes 410 can be hidden from view by application of panel 21. Further, lower panel 21 is made opaque so that these bolt holes 410h and fasteners 416 are substantially completely hidden from view when lower cover panel 21 is applied to housing 11. Because, holes 410 and fasteners 416 for holding the parts of housing together are hidden from view in the terminal of Fig. 1a, a person cannot determine the assembly

features of terminal by inspection. The unscrupulous party considering opening terminal 10 may determine from inspection that terminal 10 is held together by forces supplied other than detachable fastening devices such as bolts or screws and may therefore give up the idea of breaking into terminal 10.

As has been described herein, PIN information should be encrypted whenever it is entered into terminal 10. If PIN information is not encrypted by terminal 10, an unscrupulous party may attempt to electronically syphon the PIN information from a storage device of terminal or in a computer system located upstream from terminal in the transaction cycle depicted in Fig. 3a. Other sensitive information may be designated as secure information which is to be encrypted. For example, credit card number information, debit card number information, personal identification information, signature information, fingerprint information, retinal signature information or other information which may be designated as secure, and received by any one of user interface devices RFID 261, optical reader imaged assembly 263, fingerprint scanner 265, retinal scanner 267, unit 240, etc. may be encrypted by terminal 10. In some countries, credit card numbers are required to be encrypted.

Terminal 10 is preferably adapted so that an operating program of terminal 10 can be customized by an user-programmer, so that the characteristic of, and sequence of, e.g. prompts, other messages, menus displayed by touch screen 20 are configurable by an user-programmer. In accordance with the invention, a programmer-user may develop instructions of an operating program using a program builder system 390 as seen in Fig. 3h (typically provided by a PC as shown) and then transmits the set of instructions built using the builder system 390 to terminal 10 over breakable link 392. However, providing a programmer-user with the capacity to freely define

features of a terminal's main operating program raises the possibility that an unscrupulous user-programmer may develop prompts which encourage a customer-user to enter PIN information or other designated secure information without an encryption sequence of instructions properly being executed. The unscrupulous user-programmer may then electronically syphon the unencrypted PIN information or other secure information.

Accordingly, terminal 10 may be adapted to include a secure information entry feature which is described with reference to Figs. 2d, 2e and 2f. In accordance with a secure information entry feature of the invention, terminal 10 may include a secure information entry circuit 280 included in the embodiment shown as central processing unit 281, a program ROM 283, working RAM 282 and cryptographic firmware 285 which results in an encryption mode signal carried by line 286 being caused to change state whenever an encryption routine (executed in accordance with program instructions which may be stored in ROM 283) is called, which encryption mode signal can only be generated by calling the encryption routine. Further, in accordance with the secure information entry security feature, an indicator 287 is made responsive to the selective state changing encryption mode signal so that the indicator 287 is active only when the encryption routine is called. Preferably, firmware 285 is established so that indicator 287 is made responsive only to the encryption mode signal caused to change state by the secure information entry circuit so that an unscrupulous party cannot cause indicator 287 to be actuated in a mode other than an encryption mode. Still further, in accordance with the secure information entry security feature, in one embodiment an information message 288 is displayed on or about terminal 10 or visible by a user of terminal 10 which informs a customer-user 310 that the

customer-user 10 should enter secure e.g PIN information only if indicator 287 is active. Information message 288 is preferably substantially permanently affixed to terminal 10 so that an unscrupulous party cannot easily remove or destroy message 288. Information message 288 may be printed or formed as part of the graphics of upper cover panel frame 22f for example, or on a part of lower panel 21 visible with upper panel 22 attached. Information message 288 may also be formed on a normally visible part of housing such as with etching, stamping, immersion graphics, a sticker, etc., preferably in proximity with indicator 287.

Referring to aspects of the secure information entry feature of the invention in further detail, cryptographic firmware 281 of secure information entry circuit 280 can take on a variety of forms. In general, the term "firmware" as used herein shall refer to any hardware or software or combination hardware/software element of a processor based controller which cannot be changed by the ordinary methods and protocols available for use by a user-programmer for changing instruction of a main program of the processor based controller.

As will be discussed in greater detail herein, circuit 280 may comprise components of control circuit 210. Accordingly, it will be seen that the characteristic of cryptographic firmware 285 of secure information entry circuit 280 may vary depending on the software architecture selected for allowing reprogramming of terminal control circuit 210 (changing of instructions of the main program). Alternative software architecture which may be employed for enabling changing of instructions of a main program associated with control circuit 210 with use of a program builder system 390 are described with reference to the memory map diagrams of Figs. 2e and 2f. In one software architecture for allowing

reprogramming of terminal 10, program builder 390 builds and control circuit 210 executes a compiled program. It is preferable that program builder system 390 allows programing of terminal using high level programming instructions or with use of graphical user interface prompts wherein program instructions are built by system 390 in response to programmer-user inputs that are input into system 390 using a GUI in response to GUI displayed prompts displayed on display 390d. Accordingly, program builder system 390, may build an operating program for terminal 10 in a high level language such as C or C++ which has to be compiled into machine code for execution. A main operating program written in a high level programming language and built in system 390 can be compiled into machine code in system 390 or in control circuit 210, if control circuit 210 is equipped with an operating system. In the case that control circuit 210 executes a compiled program or an assembled program (e.g.. written in assembly code at system 390 and than assembled) cryptographic firmware 285 circuit 280 and circuit 210 may take the form as shown in the ROM program memory map as shown in Fig. 2e. As indicated by Fig. 2e several address locations 270 of program ROM 283 may be allocated for storing compiled operating program whereas other address locations 271 may be allocated for storing firmware instructions which are not affected by the compiling and loading of a new operating program on ROM 283. In the example of Fig. 2e firmware 281 refers to code instructions stored on firmware allocated address locations 290 of ROM 283. Cryptographic firmware 285 in the example of Fig. 2e may be e.g. a set of instructions which operate to poll the contents of instructions called for execution by compiled program stored in addresses 270. When a called instruction is an instruction to call an encryption routine, cryptographic firmware 285 results in an encryption mode

signal changing state.

In another architecture which may be employed from allowing reprogramming of terminal 10, circuit 210, 280 executes a script program (which is sometimes referred to simply as a script) that is built by a programmer-user at builder system 390 using high level instructions or e.g. by inputting inputs in response GUI displayed programming prompts displayed on display 390d. When circuit 210, 280 is of the type that executes a script program, ROM 283, 218 stores an interpreter program stored in address locations 270. When a script program architecture is selected, script instructions built at builder system 390 do not have to be complied into machine code prior to being executed. Instead, when a script program architecture is selected, interpreter program stored at 270 interprets and executes script instructions built at system 390 and thereby eliminates the need to compile a set of high lever instructions authored at system 390 into machine code prior to their execution by terminal 10. In the example of Fig. 2f "firmware" can be considered to include code instructions of the interpreter program stored at address locations 270 since these instructions cannot be affected by changes in the script code built at builders system 390. In addition, when ROM 283, 218 includes an interpreter program, ROM 283, 218 can include additional firmware at locations 271 of the type described with reference to Fig. 2e (i.e. memory stored instructions impervious to changes in an interpreter program). While firmware is shown in the memory maps of Figs. 2e and 2f to be included in program ROM 283, 218, it will be understood firmware can also be included in working RAM 282 or in an internal register of CPU 281.

It will be understood that the above archetypal examples are selected merely to highlight that cryptographic firmware 285 can take on a variety of different forms and are not

intended to rigorously define the precise characteristic of subject matter that can be considered firmware. In fact many software architectures exhibit characteristics of both of the archetypal architectures described. Still further it will be understood that firmware e.g. 285, while most typically comprising some form of user inaccessible or difficult to access code instructions, need not comprise any code instructions. For example, cryptographic firmware 285 according to the invention can include discreet IC formed electrical circuit components tied to an appropriate address bus location e.g. a key storing address 291 of RAM 282 or ROM 283 called during execution of an encryption routine of the invention which circuit components are operative to change the state of an encryption mode signal when such an address is selected.

As has been indicated herein and again by Fig. 2d encryption keys utilized by an encryption routine are preferably stored in battery powered volatile RAM 282 which can be erased either by an instruction or by disconnecting a battery B supplying power thereto. Accordingly, as alluded to previously in one specific example of secure information entering circuit 280, circuit 280 may include elements of both control circuit 280 and security block 220, as is indicated by reference numeral 280 of Fig. 2c and 2d.

Additional features of the invention will be understood with reference to one specific example of the invention. A flow diagram explaining operations of secure information entry circuit 280 as may occur when executing an encryption routine utilizing the two CPU architecture of Figs. 2c and 2d is described in detail with reference to the flow diagram of Fig. 2h. At block 295a CPU 212 executing instructions stored in ROM 218 of circuit 210 determines if an encryption routine has been called, e.g. by selection of a menu option of a user or

an insert and reading of a card by a user. If an encryption routine is called, cryptographic firmware 285 at block 295b changes the state of an encryption mode signal carried by line 286 from a first state to a second state to turn indicator ON. At block 295c CPU 212 causes virtual keypad to be displayed on touch screen 20. At block 295d CPU 212 captures the entered keystrokes and at block 295e CPU 212 sends the PIN information to circuit 221, and calls for the encryption algorithm stored in ROM 223 of chip 221 to be executed. At block 295f, CPU 224 of chip 221 executes this encryption algorithm using encryption keys stored in RAM 222, and at block 295g CPU 224 sends encrypted PIN information to RAM 217 of circuit 210. As indicated by block 295h, CPU 212 has been polling line 297 for received data. When data is received by circuit 210 CPU 212 changes the state of the encryption mode signal to its original state. It is seen that the above example is applicable to any other application as described herein, wherein encryption may be useful. For adapting the method of Fig. 2h for another application involving encryption of the PIN pad user prompt setup (block 295c) may be substituted for by another prompt message (a text message "Insert Card," "Place Finger on Recess," etc.).

Referring to further aspects of indicator 287 a secure information entry feature of the invention, indicator 287 may take on several forms. In the example of Figs. 1a, 1f and 4a indicator 287 is provided by an LED 287L mounted on main circuit board 290 in combination with a light pipe 287p having a distal end 287pd visible at top 11a of terminal 10 proximate touch screen 20. In one example, the changing of the encryption mode signal from a first state to a second state changes a light source indicator from an OFF state to an ON state. However, terminal 10 could be configured so that the changing of the state of the encryption mode signal from a

first state to a second state could also change the state of light source indicator from an ON state to an OFF state. When indicator 287 is a light source, the light source may be a light source other than an LED, such as a filament used light source. Indicator 287 can be provided by a changing of the control of a backlight 236 of display 234. Further, a change in the state of the encryption mode signal need not change the state of a light source indicator from an OFF state to an ON state. Terminal 10 could be adapted so that a change in the state of the secure mode signal increases the intensity of light from a first ON state to a higher intensity second state. In addition, more than one light source can be used. Still further, indicator 287 if a light source need not be located at terminal 10. A light source indicator could comprise overhead or other visible lights proximate terminal 10 for example.

Importantly, indicator 287 need not comprise a light source. Indicator 287 could comprise an acoustic output device in terminal 10 or away from terminal 10. Indicator 287 could also be a graphical icon or message displayed on screen 20 or on a display e.g. display 340 spaced apart from terminal 10. The state changing encryption mode signal (which may be encrypted by terminal 10) can be transmitted to any computer system of POS network 300, shown in Fig. 3a, and any computer system of POS network may control indicator 287. Further, hub 360 may include a program which monitors encryption mode signal data from each of several terminals 10, to maintain a record on PIN captures, and report any anomalous events (e.g., encryption mode signal state changes not corresponding to PINs captures).

Referring to further aspects of information message 280, it will be understood that the attributes of information message 288 will change depending on what secure information

is being captured by terminal 10 and the characteristics of indicator 287. In the example of Fig. 1a wherein indicator 287 comprises an LED and the secure information is PIN information, message information may be printed matter formed on housing stating "DO NOT ENTER PIN INFORMATION UNLESS LIGHT IS ON". If the secure information to be encrypted is a credit card number, and indicator is an acoustic device, then information message 288 may be printed matter which states "DO NOT INSERT CARD UNLESS TONE IS SOUNDED". In addition to or instead of being comprised of printed matter message information 288 may be electronically generated text information displayed by screen 20, permanently generated by firmware of terminal or caused by terminal firmware to be displayed by previous action of a user. Also, information message 288 need not be located on terminal 10. Information message 288 may be printed matter or electronically generated message data at a location proximate terminal, such as on a sign proximate terminal 10. Information message 288 may also include printed matter included in product literature supplied by a supplier of terminal, and may include electronically displayed messages which may be accessed by accessing a website of a supplier of terminal.

While the present invention has been explained with reference to the structure disclosed herein, it is not confined to the details set forth and this invention is intended to cover any modifications and changes as may come within the scope of the following claims.